SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

REF KDB 594280 D02 U-NII Device Security v01r03

Model:SBWD960B FCC ID: **LNQSBWD960B**

General Description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. ANS: Firmware update will not affect the radio frequency (rf) parameters. Users can not modify the RF parameters of thedevice through the device's management system.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that nay other software/firmware changes will not allow the device to exceed the authorized RF characteristics? ANS: The radio frequency parameters are pre-configured in factory. End users can not modify them.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification. ANS: The RF module firmware is provided by the RF module manufacturer. The firmware of the RF module can be updated by the firmware of the product. The firmware of the product updates itself when a known user is authenticated. It needs to login to a server to download the new firmware version. The new firmware of the product is signed and the signature of the firmware is verified before writing it to the flash The firmware product is compressed and readonly and user operation can not modify the RF firmware. The RF parameters can not be modified.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. ANS: Here is what we use for cryptography: 1. Symmetric(Secret - Key) AES: key (1)=key (2) 2. Asymmetric(private/public - key) RSA: key(1) ≠key(2) 3. Hash Function (One - Way) fixed - length output for the use in digital signature Process Plain text --- key (1) ---> Cipher text ---key (1)---> Plain text For the firmware: Encrypted with AES - 128 and signed with RSA - 1024 For hardware: Disable inputs (UART/TELNET/EJTAG)
	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation? ANS: Can not be configured as a master and client. The operation mode is fixed.
Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.

	ANS: The Wi‑Fi channels are pre-configured in factory. End users are not allowed to change. Because no interface is provided to read these data, and the data are random password protected.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/ or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality. ANS: Third-party software or firmware installation is not allowed.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization. ANS: The WiFi channel plan (frequency) isstored in the ROM on the WiFi chip. There is no interface or method to modify when the unit leaves the factory. Even the firmware/software is changed, the WiFi channels remain the original configuration.

User Configuration Guide	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. ANS: Through the UI, users can configure basic receiver information, enable/disable receiver features, update receiver firmware, receiver maintenance, etc.. The RF parameters can not be modified through the UI. No access control level is applied.
	a) What parameters are viewable and configurable by different parties? ANS: No access control level is applied.
	b) What parameters are accessible or modifiable by the professional installer or system integrators? ANS: No access control level is applied.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

	ANS: Yes. Users can only select from the available options or enter the value in the defined range.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? ANS: The software is pre-configured in factory, and the FLASH is e-fused with encryption method, please refer to Q4's answer in the General Description section. End users can not change the software or WiFi channel. And, firmware update will not change the WiFi related parameters.
	c) What parameters are accessible or modifiable to by the end-user? ANS: No access control level is applied.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? ANS: Yes. Users can only select from the available options or enter the value in the defined range.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? ANS: The software is pre-configured in factory, and the FLASH is e-fused with encryption method, please refer to Q4's answer in the General Description section. End users can not change the software or WiFi channel. And, firmware update will not change the WiFi related parameters.
	d) Is the country code factory set? Can it be changed in the UI? ANS:The country code ispre-set in factory. It can NOT be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? ANS: The software is pre-configured in factory, and the FLASH is e-fused with encryption method. End users can not change the software or WiFi channel. And, firmware update will not change the WiFi related parameters.
	e) What are the default parameters when the device is restarted? ANS: The last saved parameters will preserve after the device is restarted.
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02. ANS: No.
	3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance? ANS: can NOT be configured as a master or client. The operation mode is fixed.
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a)) ANS: The unit can NOT be configured as different types of access points.